

Euklides by się uśmieł, czyli jak można odwracać indeksy

dr Teresa Jurlewicz, Instytut Matematyki i Informatyki PWr

Michał Bryłka, Łukasz Świątkowski, Małgorzata Jurlewicz
- studenci Wydziału Informatyki i Zarządzania PWr

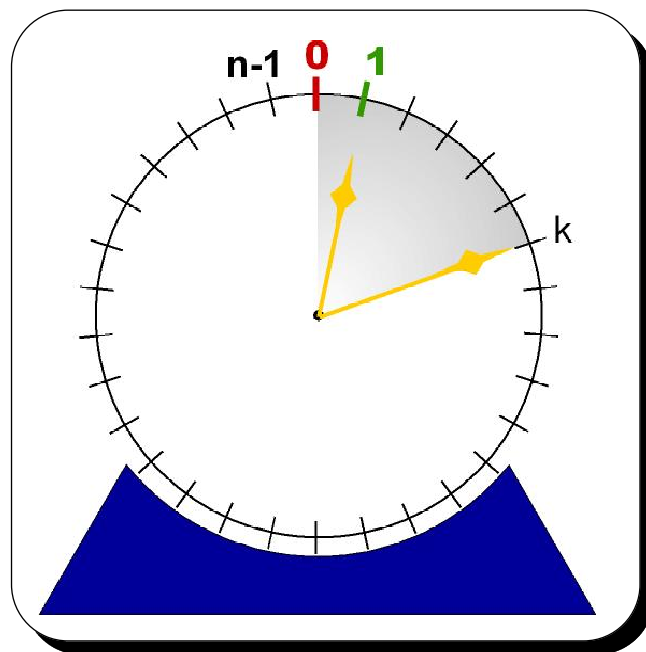
Zegar odwracający

Zegar odwracający służy do wyznaczania odwrotności w arytmetyce modularnej dla elementów pierścienia \mathbf{Z}_n reszt modulo n . W sposób poglądowy przedstawia on samą definicję tego pojęcia. Niech zatem $n \geq 2$ oraz niech $\mathbf{Z}_n = \{ 0, 1, 2, \dots, n-1 \}$. Mówimy, że liczba $l \in \mathbf{Z}_n$ jest **odwrotnością modulo n** liczby $k \in \mathbf{Z}_n$, jeżeli reszta z dzielenia liczby kl przez n jest równa 1, co zapisujemy w postaci $(kl) \bmod n = 1$. Dla pewnej liczby całkowitej m zachodzi zatem równość

$$kl = mn + 1.$$

Odwrotność modulo n elementu k oznaczamy symbolem $k^{-1} \bmod n$. Element zbioru \mathbf{Z}_n posiadający odwrotność modulo n nazywamy **odwracalnym modulo n** , w przeciwnym przypadku nazywamy go **nieodwracalnym modulo n** .

Wyobraźmy sobie teraz tarczę n -zegara z podziałką na n części ponumerowaną od 0 do $n-1$ oraz dwie wskazówki - dużą i małą. Załóżmy, że duża wskazówka n -zegara skacze o k , zaś jego mała wskazówka liczy skoki dużej. Odwrotność modulo n do elementu k wskaże nam zatem mała wskazówka w chwili, gdy duża wskazówka znajdzie się w położeniu 1. Jeżeli to nastąpi, to na pewno przed n -tym skokiem. Może to jednak nigdy nie nastąpić, ale wtedy z pewnością duża wskazówka znajdzie się przed n -tym skokiem w położeniu 0, a to oznacza nieodwracalność modulo n elementu k . Dużą wskazówkę będziemy nazywać **k -wskazówką**, zaś małą **l -wskazówką**, **licznikiem**, lub **wskazówką odwracającą**. Opisany model będziemy nazywać **zegarem odwracającym**.



Rysunek. Zegar odwracający.

Wykonanie rysunku: M. Jurlewicz.

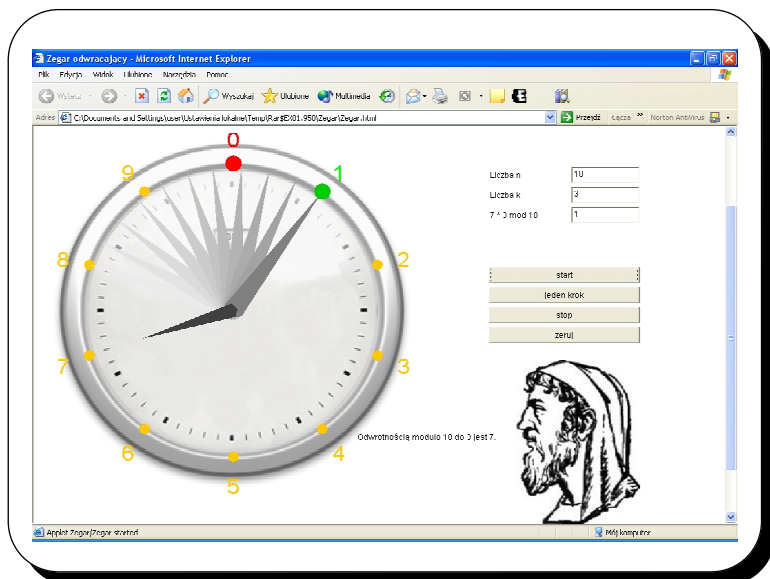
Parametry k, l, m, n występujące w równości $kl = mn + 1$ definiującej odwrotność modulo n liczby k są w zegarze odwracającym realizowane są zatem jako:

n - zakres podziałki zegara;

k - wielkość skoku dużej wskazówki;

l - liczba, którą wskazuje mała wskazówka w momencie, gdy duża wskaże 1, jest to liczba skoków wykonanych przez dużą wskazówkę;

m - liczba pełnych obrotów dużej wskazówki do momentu zatrzymania się jej w punkcie 1, tej liczby nie widać bezpośrednio na zegarze chyba, że wprowadzimy jeszcze jedną wskazówkę (tzw. **obrotomierz** lub **m -wskazówkę**).



Wirtualny model zegara odwracającego utworzył jako applet **Java** pan mgr inż. Przemysław Bieчек, doktorant Instytutu Matematyki i Informatyki Politechniki Wrocławskiej. Został on zaprezentowany na VIII Dolnośląskim Festiwalu Nauki oraz zamieszczony na stronie internetowej wykładu

www.wppt.pwr.wroc.pl/dfn2005tj

Dwa plastikowe modele zegarów odwracających modulo 5 oraz modulo 10 zostały przygotowane na wykład dzięki uprzejmości pana Jarosława Uszaka, rzemieślnika.

Teresa Jurlewicz, 21 września 2005